Cybersecurity Framework Workshop 2016
National Institute of Standards and Technology, Gaithersburg MD

April 5-7, 2016

Workshop Purpose: The purpose of this workshop is to provide attendees a broad sampling of Framework use and work products, as well as gather input to help NIST understand stakeholder awareness and current use of the Framework, the need for an update to the Framework, cybersecurity best practices sharing, as well as the future governance of the Framework.

Agenda

Tuesday, April 5, 2016 (optional)

11:15 AM **Registrant Check-In**

12:15 PM **Optional Seminar: Framework Overview**

2:00 PM **Break & Registrant Check-In**

2:15 PM **Optional Seminar: Framework Overview (repeat session)**

4:00 PM **Adjourn**

Wednesday, April 6, 2016

7:30 AM **Registrant Check-In**

8:30 AM **Welcome Plenaries and Keynotes**
Dr. Kent Rochford, Associate Director for Laboratory Programs, NIST
Alan Davidson, Director of Digital Economy, Department of Commerce

9:10 AM **NIST Panel RFI Readout**
Donna Dodson, Chief Cybersecurity Advisor, NIST
Adam Sedgewick, Senior Policy Advisor, NIST
Matthew Barrett, Cybersecurity Framework Program Manager, NIST

9:40 AM **Break**

10:00 AM **Panels**
Red Auditorium:

- **Framework Use** - This panel will focus on the individual organizational uses of the Framework

Green Auditorium:

- **US Coast Guard Maritime Profile Strategy** - This panel will focus on the work done by the US Coast Guard and partner organizations on building security profiles, based on the Framework, to secure the bulk liquid

transport sector.

11:10 AM **Panel**
Red Auditorium:
- **International Alignment -** This panel will focus on how other countries are aligning and using the Framework in their cybersecurity policy.

12:20 PM **Breakout Session Introductions and Rules of Engagement**

12:30 PM **Lunch**

1:45 PM **Working Session I**
Red Auditorium: Potential Framework Update
Green Auditorium: Roadmap – Italian National Framework for Cybersecurity as an Example of International Alignment
Portrait Room: Roadmap – Automated Indicator Sharing
Heritage Room: Potential Framework Update
Lecture Room A: Potential Framework Update
Lecture Room B: Governance
Lecture Room D: Best Practice Sharing
West Square: Roadmap – Workforce Education

3:15 PM **Break**

3:30 PM **Working Session II**
Red Auditorium: Potential Framework Update
Green Auditorium: Special Topics – Manufacturing Profiles
Portrait Room: Roadmap – Supply Chain Risk Management
Heritage Room: Potential Framework Update
Lecture Room A: Potential Framework Update
Lecture Room B: Governance
Lecture Room D: Roadmap – Assessment and Confidence Mechanisms
West Square: Best Practice Sharing

5:00 PM **Adjourn**

Thursday, April 7, 2016

8:00 AM **Registrant Check-In**

9:00 AM **Working Session III**
Green Auditorium: Special Topics – FFIEC Cybersecurity Assessment Tool
Portrait Room: Roadmap – Privacy and Civil Liberties
Heritage Room: Roadmap – Federal Agency Cybersecurity Framework Use
Lecture Room A: Potential Framework Update
Lecture Room B: Potential Framework Update
Lecture Room D: Best Practice Sharing

10:30 AM **Break**

11:00 AM **Working Session IV**
Green Auditorium: Special Topics – CSIP Recover Publication Concepts
Portrait Room: Special Topics – USCG Maritime Profile Strategy
Heritage Room: Special Topics – Research & Development Relevant to the Framework
Lecture Room A: Governance
Lecture Room B: Potential Framework Update
Lecture Room D: Roadmap – Authentication

12:30 PM **Lunch**

1:30 PM **Panel**
Red Auditorium:

- **Insurance** - This panel will discuss the benefits to an evolving and growing insurance market of a widely used and consistent approach to understanding and communicating cyber risks. Panelists will provide their experience with using the Cybersecurity Framework for developing and analyzing data and using the data for underwriting cyber risks.

2:40 PM **Panel**
Red Auditorium:

- **State and Local Use of the Framework -** This panel will bring together the states that use Framework to coordinate efforts within their jurisdictions.

3:40 PM **Readout of Workshop Findings and Next Steps**
Kevin Stine, Division Chief – Applied Cybersecurity Division, NIST
Matthew Barrett, Cybersecurity Framework Program Manager, NIST

4:30 PM **Adjourn**

Breakout Session Descriptions

Best Practice Sharing: This session aims to generate and share additional private sector insights and recommendations about how best practices for using the Framework are being shared and additional steps to increase sharing. These insights will inform NIST's decision making about future actions and could spur additional actions by others. Participants are expected to offer their views about the kinds of sharing and the degree of sharing being conducted by NIST and others. These include sharing by users of the Framework, product and services organizations, and industry associations.

Potential Framework Update: With the Framework entering its third year of existence, NIST is interested in understanding the need for a potential update. This session will include discussions surrounding the use of the Framework, what's working, and what could be updated. Participants will provide feedback regarding potential timelines for an update, the process an update might follow, and what content within the Framework needs to be updated.

Governance: NIST currently serves as the convener of Framework development activities and the manager of daily Framework activities. Through this session, NIST would like to discuss the possibility of non-Governmental parties participating with NIST in Framework leadership roles. Participants will discuss possible division of labor across Government and non-Governmental leadership, interplay between those parties to maintain and evolve Framework, and properties non-Governmental parties would need to make shared leadership of Framework successful.

Roadmap - Authentication: In light of the increasing range of critical access points to an organization's enterprise, this session will review some of the concepts stated in the Authentication item of the Framework Roadmap, and discuss the relevant current and emerging standards for user authentication and identity proofing. Desired outcomes from this session include: a list of relevant technology areas requiring standards, along with a corresponding list of currently-available material; a high-level conceptual view of how these standards relate to internal users, external users, and devices; and a discussion of how any gaps in standards can be addressed by industry consortia or standards development organizations.

Roadmap - Supply Chain Risk Management: This session will discuss NIST's work on Cyber Supply Chain Risk Management (SCRM) stemming from the NIST Roadmap for Improving Critical Infrastructure Cybersecurity. NIST will share its research and findings on industry best practices for cyber SCRM and standards mappings to the Framework and seek validation and input from stakeholders. Additionally, NIST will seek input into how SCRM fits into the Framework and future research and work needed in Cyber SCRM.

Roadmap - Federal Agency Cybersecurity Framework Use: This session is for discussing ways that the Framework can provide value to the risk management programs and practices in federal agencies. This may include ways that Framework complements RMF practices to improve an agency's risk management.

Roadmap - Privacy and Civil Liberties: This session will continue the discussion surrounding the use, benefits, gaps, and tools needed for the privacy and civil liberties methodology within the Framework. Participants will provide feedback regarding policy-agnostic tools that support privacy risk management.

Roadmap – Italian National Framework for Cybersecurity as an Example of International Alignment: The Italian National Framework for Cybersecurity was published in 2015 for comment. This document leverages and extends the NIST Cybersecurity Framework to provide the basis of a national framework for managing cybersecurity risk. This session will be a presentation of the methodology used to create the Italian National Framework for Cybersecurity.

Roadmap – Automated Indicator Sharing: The objective of this working session is to identify key practices for publishing, consuming, and using cyber threat indicators within an organization's cybersecurity program. The session will cover the ingest, use, and distribution of indicators. The session will not cover: privacy and civil liberties, liability, or other topics previously covered in other workshops.

Roadmap – Assessment and Confidence Mechanisms: This session will use presentations and facilitated discussion to explore the different types of mechanisms used by organizations to develop/increase confidence in their ability to manage cybersecurity risk. Each of the presenters will walk through key aspects of their approach that provide value to stakeholders/customers and leverage the Framework. The facilitated discussion will include the presenters and the audience to explore topics related to considerations in the development, use, and adoption of their unique approaches; the depth/breadth of the approach, the use of measures and scale (quantitative or qualitative), translational value, and organizational focus (C-suite to cyber control implementation to user).

Roadmap – Workforce Education: This session will cover the new NIST Special Publication of a cybersecurity workforce framework. The goal is to describe the overall NICE Strategic Goals & Objectives, the existence of the NICE Working Group and subgroups (K-12, Collegiate, Competitions, Training and Certifications, and Career Development & Workforce Planning) to attendee membership. Participants are encouraged to share activities, resources, and tools that are already in use to support the development of the cybersecurity workforce.

Special Topics - USCG Maritime Profile Strategy: This session will provide an overview of the maritime bulk liquid transport Framework Profile development effort between the US Coast Guard and NIST National Cybersecurity Center of Excellence. Participants will be asked for feedback on the US Coast Guard strategy in developing the Profile. After a brief introduction on the process used to develop the Profile and its structure, participants are invited to share their experiences in developing Profiles, as well as provide insight for refining the Coast Guard strategy.

Special Topics - FFIEC Cybersecurity Assessment Tool: The Federal Financial Institutions Examination Council, on behalf of its members, released the Cybersecurity Assessment Tool on June 30, 2015, to help institutions identify their cyber risk and assess their cybersecurity preparedness. The purpose of the Assessment working session is to encourage substantive input from financial institutions and other interested parties on ways to improve the Assessment.

Special Topics - Manufacturing Profile: This session will present a draft manufacturing profile of the NIST Framework. The presentation will include a project overview and the approach taken to develop the profile and its use in the NIST Smart Manufacturing Systems Cybersecurity Testbed. Facilitated discussion with the audience will explore tailoring the Framework in the manufacturing environment and the draft manufacturing profile. This session aims to receive feedback from participants in regards to the draft Framework Profile for Manufacturing. Read ahead material can be found at http://go.usa.gov/cHbse

Special Topics – Recover Publication Concepts: NIST was directed by the Cybersecurity Strategy Implementation Plan to develop a paper detailing how federal agencies can recover from a cyber incident. Recovery is one part of the enterprise risk management process lifecycle as one of the functions of the Cybersecurity Framework. This session will present the current working draft of the Recover publication. Participants are encouraged to offer best practices, tools, technologies that help in the recovery process as well as provide input into the current draft. Read ahead material can be found at http://go.usa.gov/cMnN5

Special Topics – Research & Development Relevant to the Framework: As part of the President's Cybersecurity National Action Plan (CNAP), the Administration also released the 2016 Federal Cybersecurity Research and Development Strategic Plan, which was coordinated by the National Science and Technology Council. This session will include a brief overview of the plan and facilitated discussion on a key feature of the plan, measuring the efficacy of cybersecurity risk management. The session will also explore what role Framework might play in that measurement.